Le serveur DNS

Abdelali SAIDI

abdelali.saidi@gmail.com

Plan

1. Concepts
2. Le fichier de configuration named.conf
3. Configurations types
4. Fichier de zone
5. Utilitaire rndc
6. Commandes de diagnostic et de configuration

Plan

1. Concepts
2. Le fichier de configuration named.conf
3. Configurations types
4. Fichier de zone
5. Utilitaire rndc
6. Commandes de diagnostic et de configuration

Concepts

Rôle

Le service DNS assure, principalement:

- la conversion de noms de domaine en adresses IP

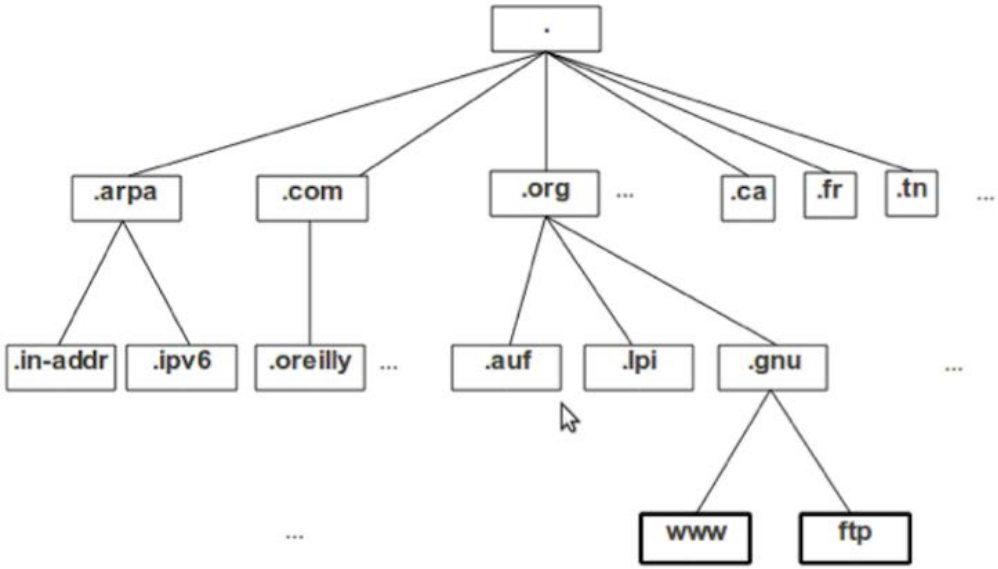
Celui d'Internet est un système distribué constitué d'un ensemble de serveurs DNS

Concepts

Domaine

- Les noms de domaines sont organisés sous la forme d'une arborescence
- les nœuds correspondent aux noms des domaines et les feuilles aux noms des hôtes

Arborescence des noms de domaine



Concepts

Domaine

- Chaque domaine appartient à un domaine de niveau supérieur et peut contenir des sous-domaines
- Au sommet de l'arbre se trouve le domaine racine
- Au premier niveau se trouve les domaines de haut niveau (TLD : Top Level Domains)
- Les TLD sont de deux types :
  - génériques (gTLD : generic Top Level Domains) tels que .com, .org, .net, etc
  - relatifs aux codes des pays (ccTLD : country code Top Level Domains) tels que .ma, .fr, .ca, .uk, .us, etc
- Au niveau Internet, les hôtes sont désignés par des noms de domaine complètement qualifiés (FQDN : Fully qualified domain name)

Concepts

Délégation

- La gestion de tous les domaines est organisée d'une manière hiérarchique
- L'ICANN (Internet Corporation for Assigned Numbers and Names) est l'organisme autoritaire du domaine racine
- Exemple : www.lpi.org
  - Ce nom de domaine se compose de deux parties: www et lpi.org
  - Le nom de domaine "lpi.org" a été délégué à une entreprise (Linux Professional Institute) par un organisme accrédité de niveau gTLD gérant ".org"
  - Ce dernier a été à son tour délégué par l'ICANN
  - La partie "www" correspond à un nom d'hôte attribué par la LPI

Concepts

Organisation et structure

- Il existe un serveur DNS à chaque niveau de la hiérarchie de délégation
- Les serveurs DNS racines (root DNS) sont sous la responsabilité de l'ICANN
- Ces serveurs doivent être connus par tous les serveurs DNS publics car ils représentent le point de départ des opérations de recherche
- Les serveurs DNS TLD (gTLD ou ccTLD) sont gérés par des agences ou des organismes accrédités

Concepts

Fichiers de zone

- Les données relatives à un domaine sont formées d'un ensemble d'enregistrements de ressources
- Ces enregistrements de ressources sont stockés dans des fichiers de zone et contiennent:
  - les données précisant le sommet de la zone et ses propriétés (SOA - Start Of Authority record)
  - les données autorité pour tous les nœuds ou hôtes de la zone (A pour IPv4 et AAAA pour IPv6)
  - les données décrivant les informations globales de la zone (tel que MX pour le serveur de messagerie et NS pour les serveurs DNS)

Concepts

Résolution de noms

Les étapes suivantes décrivent le processus de résolution du nom de domaine “www.exemple.com”

1. Le client DNS envoie la requête de résolution du nom de domaine au serveur DNS local
2. Le serveur DNS local cherche l’information dans sa table locale (cache)
3. La requête est envoyée vers un serveur racine qui renvoie l’adresse d’un serveur TLD gérant le domaine “.com”
4. La requête est envoyée au serveur TLD “.com” qui renvoie l’adresse du serveur DNS gérant le domaine “exemple.com”
5. La requête est envoyée au serveur DNS gérant “exemple.com” qui envoie la réponse vers le client DNS

Concepts

Résolution de noms

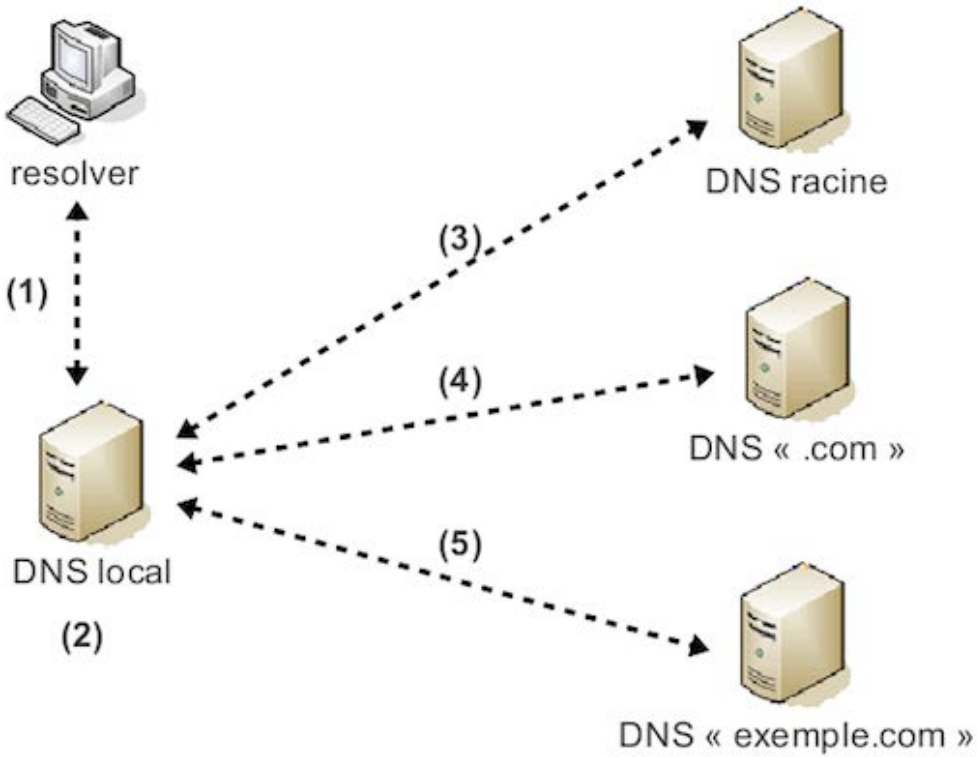


Figure : Exemple de résolution d'un nom de domaine

Plan

1 Concepts
2 Le fichier de configuration named.conf
3 Configurations types
4 Fichier de zone
5 Utilitaire rndc
6 Commandes de diagnostic et de configuration

Structure et format

Le fichier named.conf

- Ce fichier est structuré en clauses
- Chaque clause regroupe un ensemble d'instructions sous la forme d'un bloc
- Dans chaque clause, il faut respecter les règles suivantes:
  - une instruction se termine par ";"
  - un bloc d'instruction débute par "{" et se termine par "};"
- Les clauses les plus usuelles sont :
  - options : regroupe les instructions contrôlant le comportement générique ou global et ayant un effet sur toutes les zones
  - zone : définit la zone supportée par le serveur
  - logging : configure l'emplacement, le niveau et le type de journalisation
  - server : définit le comportement et les propriétés du serveur lorsqu'il accède ou répond aux serveurs de noms distants

Plan

1 Concepts
2 Le fichier de configuration named.conf
3 Configurations types
4 Fichier de zone
5 Utilitaire rndc
6 Commandes de diagnostic et de configuration

Configurations types

Il existe plusieurs manières de configurer un serveur DNS. On en trouve:

- un serveur maître
- un serveur esclave
- un serveur de cache
- un serveur de retransmission

Le serveur maître

Un serveur de nom maître définit le fichier de la zone sur laquelle il fait autorité

Exemple

```
zone "exemple.com" {
    type master;
    notify no;
    file "/etc/bind/db.exemple.com";
};
```

Le serveur esclave

Un serveur de nom esclave récupère ses données de zone moyennant l'opération de transfert de zone à partir du serveur maître et répond en tant que serveur autoritaire aux requêtes concernant cette zone

Exemple

```
zone "exemple.com" {
    type slave;
    file "/var/cache/bind/db.exemple.com";
    masters { 192.168.1.1; }; // adresse IP du serveur maître
};
```

Rectification du master

```
allow-transfer { 192.168.1.2; }; // liste des adresses IP des
                 // serveurs esclaves
```

Le serveur de cache

Un serveur de cache récupère les informations à partir du serveur maître de la zone contenant l'information et sauvegarde les données localement pendant une durée de vie (TTL)

Exemple

```
forwarders {
   10.1.1.1; //par exemple : premier serveur DNS du FAI
   10.1.1.2; //                deuxième serveur DNS du FAI
};
```

Le serveur de retransmission

Un serveur de retransmission est un serveur qui transfert toutes les requêtes à un autre serveur DNS supportant les résolutions récursives

Exemple

```
options {
        ...
        forwarders {10.0.0.1; 10.0.0.2;};
        forward only;
};
```

Plan

1 Concepts
2 Le fichier de configuration named.conf
3 Configurations types
4 Fichier de zone
5 Utilitaire rndc
6 Commandes de diagnostic et de configuration

Le fichier de zone

Rôle

Un fichier de zone contient les enregistrements de ressources d'un espace de noms. Le nom et l'emplacement d'un fichier de zone est spécifié par l'instruction file de la clause zone du fichier named.conf.

Format d'un fichier de zone

- un fichier de zone contient des commentaires, des directives et des enregistrements de ressources
- un commentaire commence par ";"
- une directive commence par "$". On en trouve:
  - $ORIGIN: définit le nom de base qui sera concaténé à tous les enregistrements non totalement qualifiés
  - $INCLUDE: inclut le fichier spécifié à l'endroit où apparaît la directive
  - $TTL: règle la valeur par défaut de la durée de vie (TTL : Time To Live) pour la zone
- le premier enregistrement de ressource doit être SOA (Start Of Authority)

Format d'un fichier de zone

Le format général d'un enregistrement est : "*nom ttl classe type valeur*" où:

- *nom* : nom (ou label) du nœud dans le fichier de zone auquel appartient cet enregistrement
- *ttl* : durée de vie (en seconde) de l'enregistrement dans un cache. La valeur 0 indique que l'enregistrement ne doit pas être maintenu dans un cache
- *classe* : définit la famille du protocole. La valeur normale est IN (INternet protocol)
- *type* : type de l'enregistrement de ressource
- *valeur* : valeur de l'enregistrement qui dépend du type et de la classe

Format des enregistrements de ressources

Types d'enregistrement de ressources

Les types d'enregistrement de ressources les plus fréquemment utilisés sont :

- SOA (Start of Authority) : définit les paramètres globaux de la zone
- A (Address): spécifie une adresse IP à associer à un nom d'hôte
- CNAME (Canonical NAME) : permet d'attribuer un deuxième nom au nom réel de l'hôte
- MX (Mail eXchange) : spécifie les noms et les préférences des serveurs de messagerie de la zone
- NS (Name Server) : définit les serveurs de noms autoritaires de la zone
- PTR (PoinTeR) : sert à la résolution inversée des noms

Format des enregistrements de ressources

SOA (Start of Authority)

Il existe un seul enregistrement de type SOA par fichier de zone et il doit etre le premier. Les paramètres qu'il peut définir sont:

- serveur : nom du serveur de noms
- e-mail : courriel du responsable du domaine
- nSerie : numéro de série du fichier de zone (à incrémenter à chaque modification)
- raf : période d'envoi des demandes de rafraîchissement par un serveur esclave vers un serveur maître
- ret : période de retransmission des demandes de rafraîchissement si le serveur maître ne répond pas
- exp : durée au bout de laquelle, si le serveur maître ne répond pas à une demande de rafraîchissement, le serveur esclave cesse de répondre aux requêtes en tant qu'autoritaire
- ttl : durée minimale que doit passer une information de cette zone dans un serveur de cache

Format des enregistrements de ressources

SOA (Start of Authority)

Le format d'un enregistrement SOA est : "nom ttl IN SOA serveur e-mail (nSerie raf ret exp ttl)". Exemple:

```
$ORIGIN exemple.com.
;name ttl classe type serveur              e-mail (nSerie raf ret exp ttl)
          IN     SOA   dns.exemple.com. root.exemple.com. (
                       2011092800 ; nSerie
                       172800     ; ou 2d ? raf = 2 jours
                       900        ; ou 15m? ret = 15 minutes
                       1209600    ; ou 2w ? exp = 2 semaines
                       3600       ; ou 1h ? ttl = 1 heure
                       )
; Les lignes qui suivent sont aussi équivalentes:
;@         IN     SOA dns.exemple.com. root.exemple.com. ( ...)
;exemple.com. IN SOA dns.exemple.com. root.exemple.com. ( ...)
```

Format des enregistrements de ressources

A (Address)

Le format d'un enregistrement A est : "nom ttl IN A ip". Exemple:

```
$ORIGIN exemple.com.
;nom      ttl classe type ip
serveur1      IN.    A    192.168.1.10
mail          IN     A    192.168.1.20
              IN     A    192.168.1.21
```

Dans l'exemple qui suit, l'adresse "192.168.1.10" est associée au nom "serveur1.exemple.com" et les adresses "192.168.1.20" et "192.168.1.21" au nom "mail.exemple.com"

Format des enregistrements de ressources

CNAME (Canonical NAME)

Le format d'un enregistrement CNAME est : "nom ttl IN CNAME nomRéelle". Exemple:

```
$ORIGIN exemple.com.
;nom ttl classe type   nomRéelle
www      IN     CNAME  serveur1.exemple.com
irc      IN     CNAME  serveur1.exemple.com
ftp      IN     CNAME  serveur.un.autre.domaine
```

L'exemple qui suit attribue les alias "www.exemple.com" et "irc.exemple.com" à l'hôte "serveur1.exemple.com" et l'alias "ftp.exemple.com" à un hôte de nom appartenant à un autre domaine

Format des enregistrements de ressources

MX (Mail eXchange)

Le format d'un enregistrement MX est : "nom ttl IN MX préférence nom".
Exemple:

```
$ORIGIN exemple.com.
;nom ttl        classe type  préfé.   nom
                IN      MX    10       mail   ;forme courte
; ceci est équivalent à
; exemple.com.  IN      MX    10       mail.exemple.com.
                IN      MX    20       mail2.exemple.com.
```

D'après l'exemple qui suit, les courriers électroniques du domaine "exemple.com" sont routés vers l'hôte "mail.exemple.com". Si ce dernier n'est pas disponible (arrêté, dérangé ou en panne) alors les courriers seront routés vers "mail2.exemple.com"

Format des enregistrements de ressources

NS (Name Server)

Le format d'un enregistrement NS est : "nomDomaine ttl IN NS nom". Exemple:

```
$ORIGIN exemple.com.
                SOA ...
;nom                ttl classe type nom
                        IN     NS   dns.exemple.com.
                        IN     NS   dns2.exemple.com.
dns                     IN     A    192.168.1.1
dns2                    IN     A    192.168.1.2
;sd.exemple.com est un sous domaine exemple.com
$ORIGIN sd.exemple.com.
                        IN     NS   dns.sd.exemple.com.
...
dns                     IN     A    192.168.2.1
;ou sans utiliser la directive $ORIGIN
;sd.exemple.com.        IN     NS   dns.sd.exemple.com.
;dns.sd.exemple.com.    IN     A    192.168.2.1
```

Cette configuration déclare les hôtes "dns.exemple.com" et "dns2.exemple.com" comme les serveurs DNS de la zone "exemple.com" et délègue la gestion du sous-domaine "sd.exemple.com" au serveur DNS "dns.sd.exemple.com"

Format des enregistrements de ressources

PTR (PoinTeR)

Le format d'un enregistrement PTR est : "nomARPA ttl IN PTR nom". Exemple:

```
$ORIGIN exemple.com.
                SOA ...
;nom                ttl classe type nom
                        IN     NS   dns.exemple.com.
                        IN     NS   dns2.exemple.com.
dns                     IN     A    192.168.1.1
dns2                    IN     A    192.168.1.2
;sd.exemple.com est un sous domaine exemple.com
$ORIGIN sd.exemple.com.
                        IN     NS   dns.sd.exemple.com.
...
dns                     IN     A    192.168.2.1
;ou sans utiliser la directive $ORIGIN
;sd.exemple.com.        IN     NS   dns.sd.exemple.com.
;dns.sd.exemple.com.    IN     A    192.168.2.1
```

L'adresse ip "192.168.1.10" sera retournée pour une recherche inversée pour l'hôte "serveur1.exemple.com"

Plan

1 Concepts
2 Le fichier de configuration named.conf
3 Configurations types
4 Fichier de zone
5 Utilitaire rndc
6 Commandes de diagnostic et de configuration

Utilitaire rndc

Présentation

L'utilitaire rndc (remote name daemon control) est utilisé pour administrer le démon named de l'hôte local ou d'un hôte distant. Il communique avec named d'une manière sécurisée à travers une connexion TCP, par défaut sur le port 953.

Le fichier de configuration de rndc est rndc.conf. Si le fichier n'existe pas, l'utilitaire utilise la clé localisée dans le fichier rndc.key

Par default, cet outil est autorisé pour les connexions locales

Utilitaire rndc

Paramétrage de named.conf

Pour les connexions distantes, il faut rajouter la clause controls au fichier de configuration named.conf.

Exemple

controls {
inet 192.168.1.1 allow { 192.168.1.20; } keys {<nomClé-192.168.1.1>;};
};

<nomClé> fait référence à la clause key du fichier de configuration named.conf

key "<nomClé-192.168.1.1>" {
algorithm hmac-md5;
secret "<valeurClé-192.168.1.1>";
};

Utilitaire rndc

Paramétrage de named.conf

Le fichier de configuration rndc.conf possède une structure et une syntaxe similaires au fichier named.conf: Il utilise les trois clauses : options, server et key.

Exemple

Le fichier de configuration rndc.conf suivant permet à l'utilitaire rndc de contrôler le démon named distant d'adresse 192.168.1.1 en utilisant la clé <nomClé-192.168.1.1>

```
key "<nomClé-192.168.1.1>" {
  algorithm hmac-md5;
  secret "<valeurClé-192.168.1.1>";
};
server 192.168.1.1{
  key  "<nomClé-192.168.1.1>";
};
```

Utilitaire rndc

Syntaxe et options

Syntaxe

La syntaxe générale de l'utilitaire rndc est :

rndc [option ...] commande [option-commande ...]

Options

Les options les plus utilisées sont :

- -c fichier : spécifie un fichier de configuration autre que rndc.conf
- -p port : spécifie un autre numéro de port
- -s serveur : spécifie un serveur autre que le serveur par défaut
- -y clé : spécifie une clé autre que celle par défaut

Utilitaire rndc

Syntaxe et options

Commandes

Les sous commandes de rndc sont :

- Halt : arrête immédiatement le service named
- Querylog : enregistre toutes les requêtes effectuées auprès du serveur de noms
- Refresh : rafraîchit la base de données du serveur
- Reload : recharge les fichiers de zone mais conserve toutes les réponses précédemment mises en cache
- Stats : vide les statistiques courantes de named vers le fichier /var/named/named.stats
- Stop : arrête correctement le serveur

Plan

1 Concepts
2 Le fichier de configuration named.conf
3 Configurations types
4 Fichier de zone
5 Utilitaire rndc
6 Commandes de diagnostic et de configuration

Commandes de diagnostic et de configuration

La commande host

Présentation

Host est une commande simple pour effectuer des recherches DNS

Syntaxe

host [option ...] nom [serveur]

- nom : le nom d'hôte ou de domaine ou l'adresse IP à résoudre
- serveur : nom ou adresse IP du serveur DNS à interroger

Commandes de diagnostic et de configuration

La commande nslookup

Présentation

La commande nslookup est officiellement abandonnée et remplacée par la commande dig. Cependant elle reste presque universellement disponible

Syntaxe

nslookup [option ...] nom [serveur]

- nom : le nom d'hôte ou de domaine ou l'adresse IP à résoudre
- serveur : nom ou adresse IP du serveur DNS à interroger

Commandes de diagnostic et de configuration

La commande dig

Présentation

La commande dig est l'outil préféré de diagnostic d'un serveur DNS

Syntaxe

dig [@serveur] nom [type-req] [+option-req ...] [-option-dig ...]

- serveur : nom ou adresse IP du serveur DNS à interroger
- nom : nom d'hôte ou de domaine ou adresse IP à résoudre
- type-req : type d'enregistrement à retourner
- option-req : précise une option de la requête ou un style d'affichage des résultats
- option-dig : option de la commande dig

Commandes de diagnostic et de configuration

La commande dig

Options

- -P : lance un ping sur le serveur à utiliser
- -p port : change le port vers lequel seront envoyées les requêtes
- -f fichier : spécifie un fichier contenant les commandes différées
- -T secondes : précise le temps entre les exécutions des commandes du fichier différé des résultats
- -c : indique la classe de requête
- -t : indique le type d'enregistrement à récupérer
- -x : spécifie que la notation inversée sera utilisée

Commandes de diagnostic et de configuration

La commande named-checkconf

Présentation

La commande named-checkconf vérifie la syntaxe d'un fichier de configuration de named ainsi que les fichiers inclus à travers l'instruction include

Syntaxe

named-checkconf [option ...] [fichier]

- nom : fichier : chemin du fichier de configuration à vérifier

Options

- -t répertoire : spécifie le répertoire racine pour un environnement enfermé
- -p : affiche le fichier de configuration named.conf ainsi que les fichiers inclus
- -z : teste le chargement de toutes les zones maîtres
- -j : lit le journal, s'il existe, lors du chargement d'un fichier zone

Commandes de diagnostic et de configuration

La commande named-checkzone

Présentation

La commande named-checkzone vérifie la syntaxe et l'intégrité d'un fichier de zone

Syntaxe

named-checkzone [option ...] zone fichier-zone

- zone : nom de domaine de la zone à vérifier
- fichier-zone : fichier contenant les données de la zone

Options

- -d : active le débogage
- -j : lit le fichier journal (cache) lors du chargement du fichier zone
- -f format : spécifie le format du fichier zone
- -t répertoire : vérifie la syntaxe du fichier dans un environnement enfermé dont le répertoire racine est répertoire